Reflection report Arctic crypt 2016
Bjørn Greve

I got funding from COINS to attend the the northernmost cryptography conference: "Arctic crypt 2016", which was held July 17-22 in Longyearbyen, Svalbard at 78 degree north. ArcticCrypt 2016 was organized by Tor Helleseth (University of Bergen), Bart Preneel (University of Leuven) and Øyvind Ytrehus (University of Bergen, simula@uib). It was a 5 day program with one full day booked for an excursion by boat to the very special place "Pyramiden" at Svalbard.

The spectacular surroundings made this trip one of the most memorable trips. The weather was not quite on our side at the start of the trip, but we got to see glimpse of midnight sun during our stay. We had a quite rough start on the trip due to missing luggage from the flight to Svalbard. Due to bad weather several flights could not land at Longyearbyen airport, which meant that both me and several of my colleagues did not receive our luggage before several days after arriving at Longyearbyen. Luckily the weather improved just in time for the conference, so that all participants could arrive safely to the conference. Both me and several of my colleagues went to Svalbard 2 days before the conference started. We helped the the organizers to set up for the conference, and also got to enjoy some of the activities offered in and around Longyearbyen. We got to rent ATVs, go fossil hunting at the end of the glacier, and we got to take a ride on a "dog-sledge with wheels. Also we went for several hiking trips in the nearby mountains. In the middle of the conference, we went a full day sightseeing, where the organizers of ArcticCrypt had booked a full day excursion to the Russian city called Pyramiden. The trip was by boat along the coast of Svalbard, going north to Pyramiden. We got to see some whales, a lot of birds and very nice nature. The attached photo is taken onboard this boat. A noteworthy fact about Pyramiden is that it was abandoned in 1998, and was empty for 9 years. However, the Russians re-populated the city, and there are now around 30 workers at a hotel there, working in cycles.

Despite having a limited capacity of facilities, the workshop attracted a wide variety of invited and submitted presentations (probably due to its exotic location). The conference consisted of about 30 talks in total, where 10 of these where invited tutorial talks on several cryptographic topics:

- Codes and stream ciphers, Symmetric cryptology.
- Homomorphic encryption.
- Privacy-friendly protocols.
- Midnight lectures.
- Authenticated encryption.
- Postquantum cryptography and Efficient implementations.
- Public key cryptography and Digital signatures.
- Side channel attacks.
- Chaining and sharing.
- Block ciphers
- Information theoretic approaches to digital security.

I think the highlight of the conference was during the midnight lectures of Adi Shamir on "How Can Drunk Cryptographers Locate Polar Bears" and Ronald R. Rivest "Symmetric Encryption based on Keyrings and Error Correction" which was very interesting, and even the midnight sun shined through the windows of the conference room during these talks. First it was Ronald R. Rivest's talk, where he discussed how to use a set of words as keys instead of a random string. After that Adi Shamir's talk, where he presented a low memory needle in a haystack problem", together with a variation of the Pollard-Rho algorithm.

For me and my Ph.D work, the most interesting talks was the following:

(1) NTRU prime, by Dan Bernstein. Related to post-quantum crypto and how we should not trust provable security. The DL problem and how factorization can be broken given access to quantum computers, which implies that it is not secure to blindly base security on the hardness of these problems.
(2) Post-quantum crypto and side-channel attacks – getting ready for the real world, by Tanja Lange. How post quantum safe algorithms should be introduced into real world applications, and also suggestions and recommendations on how the primitives could be implemented.
(3) Generic security of full-state keyed duple, by Joan Daemen.
(4) Some new results on QC-MDPC Codes and stream ciphers, by Thomas Johansson. QC-MDPC=Quasi-Cyclic Moderate Density Parity Check Code. A cryptosystem which is a code based encryption scheme, like the McEliece Cryptosystem, that use a p-alphabet instead of a binary alphabet.
(5) Symmetric Cryptography for New Applications, by Christian Rechberger. Particularly interesting since I am working within this field at the moment.

Among the papers submitted to the conference, the following papers was interesting:

- An analysis of a homomorphic encryption scheme, verifying the validity and giving a presentation of three attacks.
- Quantum crypto; assuming quantum computers exists, but communication is still sent as normal signals.
- Security analysis of BLS and BGLS signatures in a multiuser setting. The multiuser setting covers the setting where the sender encrypts, under different keys and plain-texts that is related to one another.

Overall the Arctic crypt conference was a very nice event which really motivated my Ph.D work. I got to meet old and new friends within cryptography, and I also got to discuss some important problems within my research with the top researchers in cryptography, which gave a lot of new ideas and approaches which help me a lot in my work. Also meeting the famous people within the field of cryptography really inspired me to work harder. It is definitely one of the most social conferences I have been to, and I would strongly recommend anyone who gets the opportunity to visit Svalbard to do so and enjoy every second of it. If there will be another Arctic Crypt, would strongly encourage all researchers within cryptography to go there if possible. I am deeply grateful for COINS supporting me to go to Arctic Crypt 2016.